Direct Connect Resources in Cornell AWS Accounts

Introduction

This document provides details about the resources in Cornell AWS accounts that support the 2023 (v2) Direct Connect architecture.

Terminology

We use the following terminology in this document:

- customer – Cornell AWS account owners/administrators
- VPC – Virtual Private Cloud
- DC – Direct Connect
- TGW – Transit Gateway
- AZ – Availability Zone

Resources

Secondary VPC CIDR Block

Each Cornell AWS VPC connected to the 2023 (v2) DC architecture has a small secondary CIDR block added to it. This CIDR block is exclusively used for for DC utility subnets (see below). The secondary CIDR block is a chunk of officially allocated Cornell private network.

Each secondary CIDR block is either **/26** (64 addresses) or **/25** (128 addresses) in size, depending on the number of AZs used by the VPC.

⚠️ Any CIDR ranges within the secondary VPC CIDR block not allocated to the utility subnets are reserved for future use by CIT.

Utility Subnets

The sole purpose of these subnets is to provide a location for TGW attachment. One utility subnet exists in each AZ that a DC-connected VPC utilizes (for standard subnets).

Each subnet is **/28** (16 addresses) in size (the smallest size allowed by AWS) and utilizes a CIDR range from the secondary VPC CIDR block. Each of the utility subnets is attached to the TGW.

Utility subnets are named using the following template: **tgw-utility-subnet-${REGION}-${AVAILABILITY_ZONE}-do-not-use**

> ⚠️ Do not deploy resources to these utility subnets. The routing of these subnets is configured to support only TGW attachments. These subnets will not work like other VPC private subnets.

Route Tables

Utility Subnet Route Table

The Route Table used exclusively by the utility subnets contains only local routes for the primary and second VPC CIDR blocks. Do not use this Route Table for other subnets.

This Route Table is named using the following template: **tgw-utility-rt-for-${VPC_ID}-do-not-use**

Customer Route Tables

Customer Route Tables support inter-VPC traffic as well as private Cornell, public Cornell, and internet network traffic. Routes in these tables direct traffic bound for the private Cornell network (10.0.0.0/8) and (optionally) public Cornell subnets use the Transit Gateway Attachment as their destination.

Customer Route Tables will have routes to the Cornell private network (i.e., 10.0.0.0/8) that use the Transit Gateway. Optionally, customer Route Tables can include routes to public Cornell IP CIDR blocks (e.g., 128.84.0.0/16) that use the Transit Gateway. ⚠️ Be aware that routes to public Cornell IP CIDRs can trigger asymmetric route problems. See Cornell AWS Direct Connect Routing Diagrams for more information.

Utility Subnet Network ACL

The utility subnets exclusively use a NACL created especially for them. This NACL allows all inbound traffic to and outbound traffic from the utility subnets.

The utility subnet NACL is named using the following template: **tgw-utility-nacl-for-${VPC_ID}-do-not-use**

Transit Gateway Attachments

Transit Gateway Attachments are the mechanism that connect VPCs to Transit Gateways and the DC infrastructure. A single TGW Attachment is made per VPC, and the Attachment is made to all utility subnets in the VPC. Importantly, a TGW attachment must be made to one (and only one) utility subnet in each of the AZs used by the VPC.

TGW Attachments are created in collaboration with the Cloud Team and connect to one of the set of TGWs used by CIT to offer Direct Connect services.

> If you plan to expand the footprint of your VPC by adding additional subnets in additional AZs, be sure to loop cloud-support@cornell.edu into your plans. We will need to ensure that utility subnets are created in each new AZ and that the TGW Attachment is extended to include the new utility subnet(s). Without this expansion you run the risk of losing connectivity between the TGW and the subnets that reside in the new AZs.

Details of TGW Attachments:

- Name template: **${VPC_ID}-to-cu-cit-network-${REGION}**
- Resource type: VPC
- DNS support: enabled
- IPv6 support: disabled
- Appliance mode support: disabled
- Tags
    - "Cost Center" = "R524755"
        - ⚠️ This will shift the hourly TGW connect charges to CIT. Do not change this!

References

- 2023 Cornell AWS Direct Connect Architecture Migration
- Cornell AWS Direct Connect
- Cornell AWS Direct Connect Routing Diagrams
- Cornell AWS Direct Connect Architecture